

What is claimed is:

1. A method for generating and verifying an ID-based  
blind signature by using bilinear parings, comprising the  
5 steps of:

generating system parameters, selecting a master key,  
and then disclosing the system parameters by a trust  
authority;

10 generating a private key by using a signer's identity  
and the master key, and then transferring the private key to  
the signer through a secure channel by the trust authority;

receiving and storing the system parameters by a user  
and receiving and storing the system parameters and the  
private key by the signer;

15 computing a commitment by using at least one of the  
system parameters, and then sending the commitment to the  
user by the signer;

blinding a message by using the commitment and a  
public key based on the signer's identity, and then sending  
20 the blinded message to the signer by the user;

signing the blinded message by using the private key,  
and then sending the signed message to the user by the  
signer;

25 unblinding the signed message by the user; and  
verifying the signature by the user.

2. The method of claim 1, wherein the system parameters include  $G$ ,  $q$ ,  $P$ ,  $P_{pub}$ ,  $H$  and  $H_1$ , where  $G$  is a cyclic group,  $q$  is  $G$ 's order,  $P$  is a generator of  $G$ ,  $P_{pub}$  is the trust authority's public key described by  $P_{pub} = s \cdot P$ , where  $s$  is the master key, and  $H$  and  $H_1$  are hash functions, respectively, described by  $H: \{0,1\}^* \rightarrow Z_q^*$  and  $H_1: \{0,1\}^* \rightarrow G$ , where  $Z_q^*$  is a cyclic multiplicative group; and
- the bilinear paring  $e$  is defined by  $e: G \times G \rightarrow V$ , where  $V$  is a cyclic multiplicative group of the order  $q$  and uses the cyclic multiplicative group  $Z_q^*$ .
3. The method of claim 2, wherein the public key  $Q_{ID}$  is described by  $Q_{ID} = H_1(ID)$ , where  $ID$  is the signer's identity, and the private key  $S_{ID}$  is described by  $S_{ID} = s \cdot Q_{ID}$ .
4. The method of claim 3, wherein the commitment  $R$  is described by  $R = r \cdot P$ , where  $r$  is a random number the signer chooses.
5. The method of claim 4, wherein the blinded message  $c$  is described by  $c = H(m, e(b \cdot Q_{ID} + R + a \cdot P, P_{pub})) + b \pmod{q}$ , where  $m$  is a message to be sent and  $a$  and  $b$  are blinding factors belonging to  $Z_q^*$ .
6. The method of claim 5, wherein the signed message is described by  $S = c \cdot S_{ID} + r \cdot P_{pub}$ .

7. The method of claim 6, wherein the step of unblinding is performed by using formula  $S' = S + a \cdot P_{pub}$  and  $c' = c - b$ .

5

8. The method of claim 7, wherein the step of verifying is performed by using following equations:

$$H(m, e(S', P) \cdot e(Q_{ID}, P_{pub})^{-c'}) = c'.$$

10 9. An apparatus for generating and verifying an identity-based blind signature by using bilinear parings, comprising:

means for generating system parameters, selecting a master key, and then disclosing the system parameters by a trust authority;

15 means for generating a private key by using a signer's identity and the master key, and then transferring the private key to the signer through a secure channel by the trust authority;

20 means for receiving and storing the system parameters by a user and receiving and storing the system parameters and the private key by the signer;

means for computing a commitment by using at least one of the system parameters, and then sending the commitment to the user by the signer;

25 means for blinding a message by using the commitment and a public key based on the signer's identity, and then

sending the blinded message to the signer by the user;

means for signing the blinded message by using the private key, and then sending the signed message to the user by the signer;

5 means for unblinding the signed message by the user; and

means for verifying the signature by the user.

10. The apparatus of claim 9, wherein the system  
10 parameters include  $G$ ,  $q$ ,  $P$ ,  $P_{pub}$ ,  $H$  and  $H_1$ , where  $G$  is a cyclic group,  $q$  is  $G$ 's order,  $P$  is a generator of  $G$ ,  $P_{pub}$  is the trust authority's public key described by  $P_{pub} = s \cdot P$ , where  $s$  is the master key, and  $H$  and  $H_1$  are hash functions, respectively, described by  $H: \{0,1\}^* \rightarrow Z_q^*$  and  $H_1: \{0,1\}^* \rightarrow$   
15  $G$ , where  $Z_q^*$  is a cyclic multiplicative group; and

the bilinear paring  $e$  is defined by  $e: G \times G \rightarrow V$ , where  $V$  is a cyclic multiplicative group of the order  $q$  and uses the cyclic multiplicative group  $Z_q^*$ .

20 11. The apparatus of claim 10, wherein the public key  $Q_{ID}$  is described by  $Q_{ID} = H_1(ID)$ , where  $ID$  is the signer's identity, and the private key  $S_{ID}$  is described by  $S_{ID} = s \cdot Q_{ID}$ .

25 12. The apparatus of claim 11, wherein the commitment  $R$  is described by  $R = r \cdot P$ , where  $r$  is a random number the

signer chooses.

13. The apparatus of claim 12, wherein the blinded message  
c is described by  $c = H(m, e(b \cdot Q_{ID} + R + a \cdot P, P_{pub})) +$   
5  $b \pmod{q}$ , where  $m$  is a message to be sent and  $a$  and  $b$  are  
blinding factors belonging to  $Z_q^*$ .

14. The apparatus of claim 13, wherein the signed message  
is described by  $S = c \cdot S_{ID} + r \cdot P_{pub}$ .

10

15. The apparatus of claim 14, wherein the means for  
unblinding unblinds the signed message by using formula  $S' =$   
 $S + a \cdot P_{pub}$  and  $c' = c - b$ .

15 16. The apparatus of claim 15, wherein the means for  
verifying verifies the signature by using following  
equations:

$$H(m, e(S', P) \cdot e(Q_{ID}, P_{pub})^{-c'}) = c'.$$

20